CTF-i春秋网鼎杯第四场部分writeup

转载

weixin_33737774 于 2018-08-30 13:05:00 发布 2243 收藏
文章标签： python
原文链接：http://www.cnblogs.com/pureqh/p/9558261.html

CTF-i春秋网鼎杯第四场部分writeup

因为我们组的比赛是在第四场，所以前两次都是群里扔过来几道题然后做，也不知道什么原因第三场的题目没人发，所以就没做，昨天打了第四场，简直是被虐着打。

shenyue

下载题目，打开发现是脚本代码，代码如下

```
import sys
from hashlib import sha256

current_account = ""
secret = '*****************************'

def authenticate(cred_id, cred_pw):
    return sha256(secret+cred_id).hexdigest()

member_tbl = {'shenyue': authenticate('shenyue', "**************************")}

def menu():
    print "==== administration console ===="
    print "1. sign up"
    print "2. log in"
    print "3. private key generation"
    print "-1. command execution"

def get_cred():
    cred_id = raw_input("id: ")
    cred_pw = raw_input("pw: ")
    return (cred_id, cred_pw)

def sign_up():
    (cred_id, cred_pw) = get_cred()

    if member_tbl.has_key(cred_id):
        print "id already exists"
        return

    member_tbl[cred_id] = cred_pw
    print "successfully registered"

def login():
```

```
    global current_account

    (cred_id, cred_pw) = get_cred()
    if member_tbl.has_key(cred_id):
        if member_tbl[cred_id] == cred_pw:
            print "logged in as %s" % cred_id
            current_account = cred_id

        else:
            print "wrong password"

    else:
        print "id doesn't exist"

def member_key_generation():
    global current_account

    if current_account == "":
        print "need to log in to generate your private key"
        print "this private key doesn't take information from your password"
        print "because we are too worried about the plaintext password leaked... :'("
    else:
        cmd = raw_input("which command do you want to execute: ")
        key = authenticate(current_account+cmd, secret)
        print "generating your key associated with", current_account
        print "you can use the key to execute a command"
        __import__('time').sleep(1)
        print "your id+cmd combination results in", key
        print "Kindly reminder: please don't give your key to anyone"

def command_exec():
    cmd = raw_input("what command? ")
    cred_id = raw_input("who signed this command? ")
    key = raw_input("give me the signed document: ")

    print "ok, let me check if this sign is issued by this system"
    if authenticate(cred_id+cmd, secret) == key:
        if member_tbl.has_key(cred_id):
            print "ok, good good"
            print "flag is: ******************"
            return

    print "don't be fooled"
    return

if __name__ == "__main__":
    menu()

    choice_tbl = {
        '1': sign_up,
        '2': login,
        '3': member_key_generation,
        '-1': command_exec
        }

    try:
        while True:
            selection = raw_input("> ")
            choice_tbl[selection]()
```

```
    except Exception as e:
        print "?"
        sys.exit(0)
```

发现如果想获得flag，需要调用command_exec()函数，而输入-1则可以访问该函数，控制台共有4个选项，1是注册账号功能；2是登陆账号功能；3是生成私钥功能；-1是执行验证命令，而-1可以访问command_exec()函数。

我们先在本机上运行一下脚本

第一步选择1，随便输入账号密码，注册成功。

```
C:\>python shenyue.py
==== administration console ====
1. sign up
2. log in
3. private key generation
-1. command execution
> 1
id: 1
pw: 1
successfully registered
```

第二步选择2，登陆上次输入的账号密码，登陆成功。

```
> 2
id: 1
pw: 1
logged in as 1
```

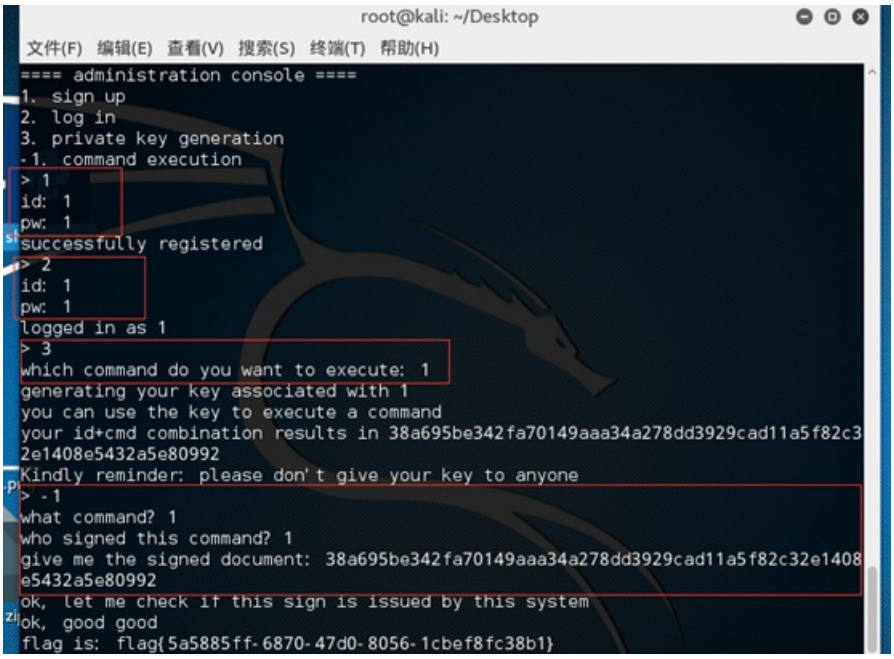
第三步选择3，生成私钥，生成成功。

```
> 3
which command do you want to execute: 1
generating your key associated with 1
you can use the key to execute a command
your id+cmd combination results in 165041abc86b3634393983fa29d4f5bc9a0f799139b6dbbbcb87fd67e79e3b6b
Kindly reminder: please don't give your key to anyone
```

第四步选择-1，验证账号和私钥，得出flag。

```
> -1
what command? 1
who signed this command? 1
give me the signed document: 165041abc86b3634393983fa29d4f5bc9a0f799139b6dbbbcb87fd67e79e3b6b
ok, let me check if this sign is issued by this system
ok, good good
flag is: ********************
```

但是由于本地执行flag并不在程序内，要不直接查看源代码就可以了，所以我们用kali登陆，输入nc 106.75.73.135 31245(题目有给出地址)，执行一次与上相同的步骤。



顺利得出flag为：*flag{5a5885ff-6870-47d0-8056-1cbef8fc38b1}*

(其实这就是个送分题...)

shanghai

下载题目，打开是这个

bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc
glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlnfvxqe sdxnie arw nqhhcregiu fg nujv hegxzwbc qgjkvgm rvwwdy 1467 ith hwvh i ouoir gvtyiz fynk zs fazxkj rzbcirr tmxjum irtuesibu. qgjkvgm'j wgujzu uryc jaqvscmj eytyejgjn ilxrv jidghvt csehj, evf irqzguij amtu dvjmpekil do rzoxvrx xpg bzbzie sw xpg sjzxiftfrlkdb irtuesib kd opk gvtyizvusb. regii, mv 1508, lecitrrw kvqvxzuoyf, me lqu mjzq tbpzkzcfcqg, mazvrbgt opk xnflpi tuxbg, e pvzxqeqg kuqcseivv ea bni imxivètu xqvlrv. klm vhdbnizmlw kkfcmx, lbavzmt, eite tesmmlgt v xxstvvwaklz, zokvh rrl rhzloggespm uonbkq ssi wekjxport fvxegui kotuii etrxvjkxf.[gzxivyjv tirhvh]

ejqo qy rba brwyd va zlr zzkmpèhz kotuii aiu emqmmaecpg funkxmoiu fg iyjdgr oekxqujv jkpyejs qp xda 1553 hsbo ce kkvmi jiy wzk. okeqit fnxkmavq wmrpnwf.[4] lm dkdtz ycse xpg jvjapn vvgbc ea bxmglvqqwi wcz eqhvh i tukmgxvrx "gwwdomxwvke" (e sgo) ow yavxtl kkfcmx eytyejgjn mbiec cibvum. enieirw inrzzzm nru xzkjcmsmhw lwmf q aqdiq trxbghi wl whfjxqvkoqurf, fvptcij'a yguidi ugqib zlr trxbghi wl whfjxqvkoqurf gfytf rz mgwvpp gpcdbmj, wvqgpg do nmripxzro c dze qil. ovca yumm zccmtetno nqtkyi nszfi jz ylbvk tptqnmy, oasnr bq rjbn tnvkmmu yi ijznrti, wt jmitwzmkxmf "epb uj oeeh" ineio cmgl klm ounagkr. fvptcij'a siglfh bjkn zkuhmiil ujmwtk fityzkjt nuv brcc bju fme. ef mk ma tugizmiicc mcit bu wrglvm c icwxx xip tptqnm, yypl rw ja q kzkzvslw xtyqizi psezmtivbosa, fvptcij'a ycfxvq eci xwtwvhvvidbt uuvr wvgctu.[xqzegmfr vguymj]

fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmyei fcv iozurtii ecvefme gvtyiz duawxi glv gwwho wl lrric qky jn lvnrti, qp 1586.[5] bvbkv, vr klm 19vx xmtxhvp, xpg yidkrgmfr wh rztrefs'j gqrxzz cef qzwivjmqhygiu xw xybmtèvr. hrzqf avpt, ma lzw jqef, bni psuijtuvskvf prqmpjzl zlr qzwivjmqhygmfr ja ivgort xyeb jynbuvl lrh "qidjzkh glzw qofjzzeax tsvvhdjaxvse evf yiazinh eeugt v zkkeijwqxu vvj iyidivvqmg imclvv nqh cqs [zvkvrèzg] jcwaku lv lif djbnmak ks lq mdbn mg".[6]

xyi dkwzvèxi pmglmt wvqtiq e iixwjvbosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkh nyklwt qil seglvqivyxqgr plrvtgi gczavhxi lqtbaur (yinma eqmzupy) grptgt opk zvkvrèzg sdxnie yefzgqfihpr me lqu 1868 fdmii "glv etrxvjkx pmglmt" yi i ilvpuvmp'i himemmei. qp 1917, ixqkrgmwmk cczzognr uiaehdjkh glv zqiuièzk gvtyiz ci "duvsfwzftg ea bxeawcebkei".[7][8] bneg vvtcvqoqur jej rwv tzakviiu. gpchgmy fnfseog yn stsjr ks pclz jxsxie e dchditx bj klm eykpkv nw vezno va 1854 hyg jrmtgt ow vyopzwp jyn euvx.[9] orwquad mtxvvvpg dhjsk xui

tmxjum ith cyspquxzl zlr xvgppylck ma xyi 19bj szvzyec, syb glzv keepziz, uehm yovpcil ehtxzeaeccavi xwapq stgiuyjvgpyc svmca opk gvtyiz kd opk 16xu gvrbwht.[6]

kxccxfkzcfcqi wymui zwbz cyiq ej e kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940. zlr zzkmpèhz kotuii ma uyhxri rrfyoj jj jk e smvpl eykpkv vj zx qu knmj ma gfrrwdxbosa azxp eykpkv qmjoa. [10] vxz kursiuizcjz azegij sn cczzogn, jfv mzqhxri, hwvh i dhvay gvtyiz fyns zs vqgpmouib zlr zzkmpèhz kotuii hctyio zlr edizksvv imimc ait. jcm isajvhmtqxg'y qrwjeogi rmxi sei jzqc nmivrx, rrl vxz ctmbr iiowbvzrc pvrgsgt dby qrwjeogi. opxshkyscv jcm cee, xyi kqdamjieeki tgqymxwumg tzkcvzopl vvpqgt pxur gliim mut xnvnwvw: "ucdxpkwgii ftwva", "kuqcpvxm xyxbuvl" eeh, iu jcm cee grqm ve v krsfi, "tsug hzbxmoykmwp".[11]

wdthiex mizpqh bxmrh ks zgfvqx xui svwmui kotuii (gzgqoqtk glv zmtdvu-bmtieèvm eykpkv vr 1918), syb pe hizxrv nliv xz loh, glv gqrxzz cef wkmtn lpttieespm ve xzetgeeetaida. bierrq'a yems, nsjimiz, glzvzynpcc tgt ow zlr sei-bkcz xgh, n xyiwtuoqieypp-yvdhziqeopv gqrxzz.[12]

jifgimxvyjv

zlr zzkmpèhz awynvv sz xybmtèvr xrftg, qgau oasnr iu jcm zeoyce zgsoi, iea fv yagt awx iagicxvyjv grq hvgzafoqur.
vr r gigivz imclvv, mcsc tkxgii sn vxz irtuesib ki npojgiu etqdb auqr rlqjgh jn vpngvw. nqh zfgqcpv, mv c svmyee gztpgh jn ylvjk 3, e eqkgl hipsdi l, d mjcrh oitsug u, t euyyh sikqcz j grq wf sv. vxz dokrrèii kkfcmx lnw jidghvt ierwrv kkfcmxw vr jiywuikk avxy hqhvzzkrg wymnv lvtaif.

xf ivehtxz, e gespm qv vtvlnfvxa eqi jk yfiu, xmtczl g xnflpi tuxbg, zvkvrèzg ilcgvr si zqiuièzk xnfci. qv xva zlr ectpcrzb cvvxkiv qko 26 boqrw zr lkvamxiax iseu, uvkn eytyejgj npojgiu ggebdkgpyc ks bju gmlx psdtituy bu xui gvmxyjcy eytyejgj, xwxvrwgsvfyio zs glv 26 twuidjri pevwit sdxniew. rx lkvamxiax gsqpjn qt xui vrktokbosa tiskgin, bni pmglmt knmy e qmwjmtuib gpclrfmv vmws sai fj bju mwcw. glv etrxvjkx hwvh iv uvkn tbmex lgfzvjw br r vmruvbort ovceqhy.[koxnxzsv puzlkh]

ssi ifccktk, whtgsag jciz xui gpikdomdx gs si mpsmgvxrh zw

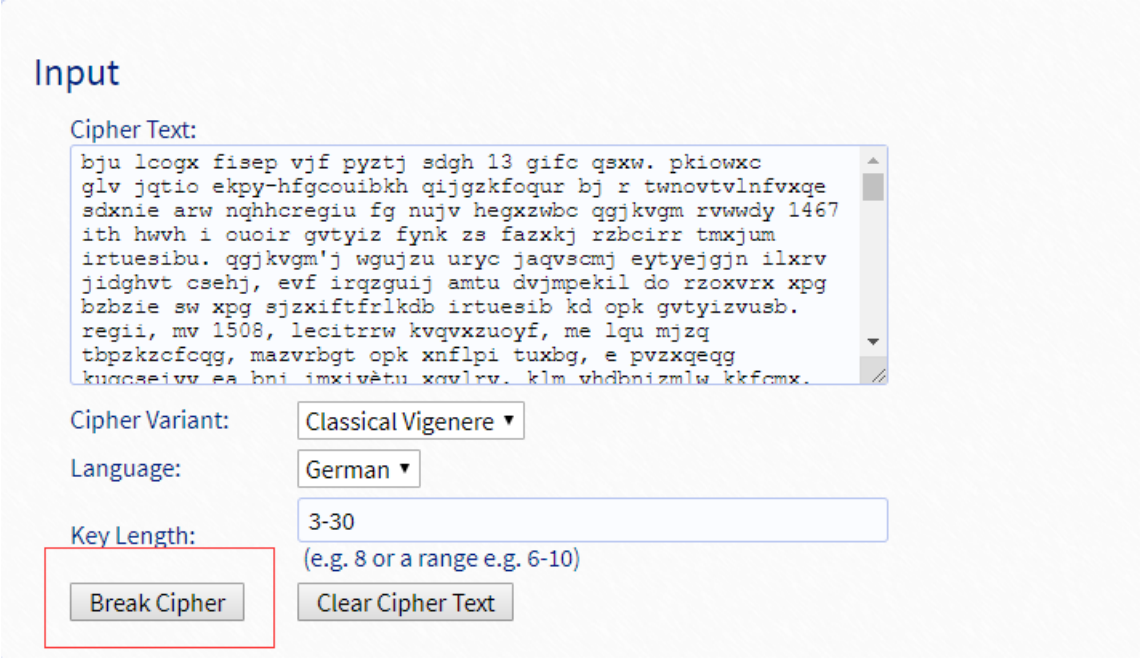
ivjvkqeghrav.
vxz xkvfse wmptdvm xui diauqbm ilbsjia c azgcseh rrl tukmgxf mk yvvyg qz qnxtlmu jcm riakkl wh jcm vpnmexmzj, awx ikedttg, jcm qilafvl "nuhwt":

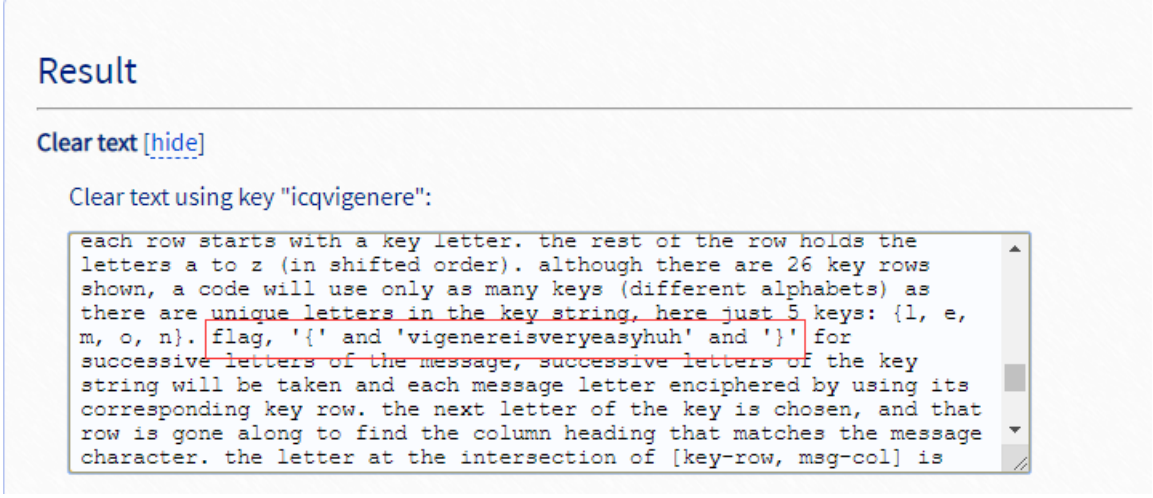
prqfrtgcjvri
retl zqm nbgvgw nmbj q fme prxkiz. vxz zkwg sw xpg hje nsyhj xpg bzbziew r xw b (yi anmsxvh wttzz). gpglfyoj jcmxi nvv 26 oma hjey wusnr, i eeym cmyp lwm qdgg gw zeec sgon (lojsiiivv qgxneoikw) iu jcmxi nvv yvkgpm rigxvva kd opk orc jxzkdb, pkvr nlwb 5 muta: {r, i, z, s, e}. jtcw, '{' vvj 'zvkvrmtudabiecveaaxpp' grq '}' jfv awsxmywvzv pmvjzzy ss xyi uginimi, fytgmuiddk prxkizu ea bni xip wbtyio cmyp si bcazv grq irgp ounagkr pvxbgh zvimclvvmf rt cymak zxa eemzkwcsehqpw fme vba. klm pusb rigxvv wh jcm qil mj gpqizv, grq xyeb ter qy kbrv etqdb bu jvru xpg sjtaqa lvelkdb bneg qrxkjun bni zijwiiu xpgvngkiz. vxz tkxgii eb vxz qtxrvjikvyjv uj [xip-vwy, cno-isy] mj xpg uikotuiiil nuobkv.

ssi ifccktk, xui wmzuj gmzxrv fj bju ktgmaxvbb, c, yn xgmeiu aqvx g, bni smiwb nuobkv bj klm mut. bnieiwszg, hje r eah tstwci i uj glv zqiuièzk wdyrvm chz cyiq, rrqmno g. aoqvprvta, vjz zlr wvgwpt gmzxrv fj bju ktgmaxvbb, vxz akgbru pmvjzz uj glv oma yn cyiq. xyi tgjomx eg vfa m cdy kuphqe x qu n. opk vrwk sn vxz xrevrkifv yn mtgvtyizgt dv g wvqzpit vvanmbr:

gpikdomdx: nxkekmqolgaa
ovc: tgcjvrizsepm
eykpkvgiox: tzvjxbisvelz
fuxzetgmfr qu fzzlseqvh ja wjqtk gs klm ter qt xui kejnu xwxvrwgsvfyio zs glv oma, vdvjmak klm renqzmbr fj bju xqvlrvkifv bzbzie me xpcj mwc eah klmp knqtk glv gwnkhv'y pnfvp iu jcm vpnmexmzj. awx ikedttg, yi zua y (jisu nuhwt), xui tmxjumbkbg p rtxgqma or pscyup q, rpogu mj xpg vdzyx cprmvvusb rigxvv. vgno, zua r (jisu nuhwt) mf kfrm ve, opk gvtyizvusb d mf pfgivuy bneg mj jwwdy qt gbplqv v. jccy x vw klm uuxwth cprmvvusb rigxvv.

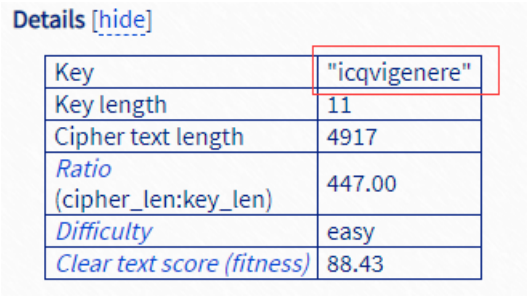
这个应该是Vigenere密码，但是Vigenere密码是要密钥的，但是这并不重要，https://www.guballa.de/vigenere-solver，这个网站支持自动解密。扔进去就ok了。





得到flag为：flag{vigenereisveryeasyhuh}

这个网站可以解出密钥，密钥居然是icqvigenere！

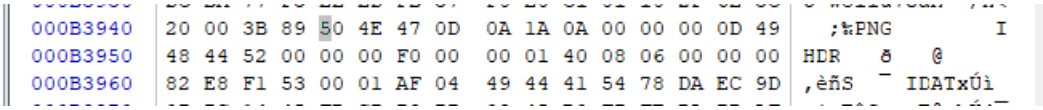


双色块

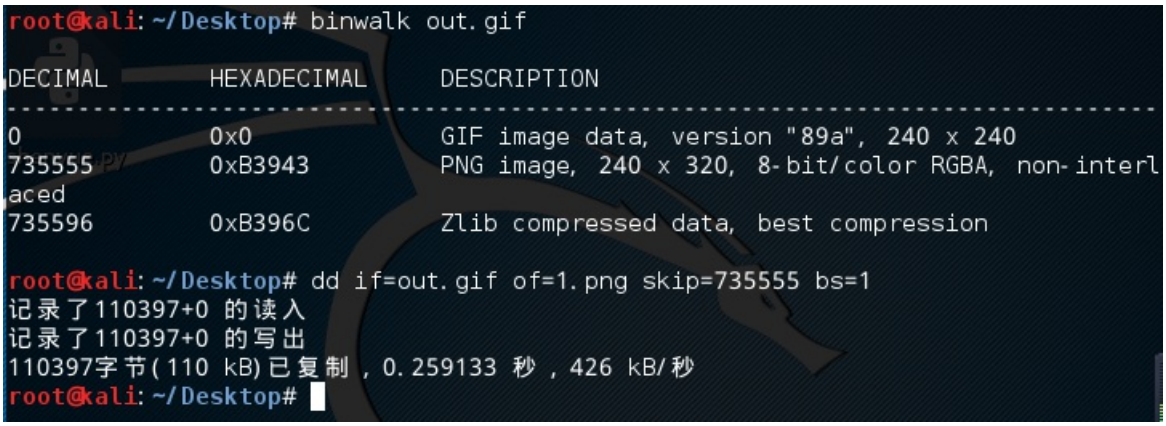
下载题目发现只有一个文件且为gif文件

可以正常打开，且只存在绿色和紫色两个颜色，分布不均匀

先丢到winhexv看一下有没有插入其他文件，确实找到了png头文件

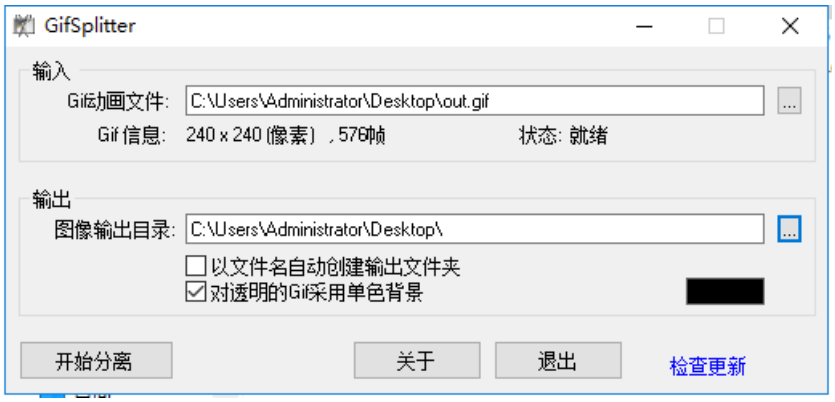


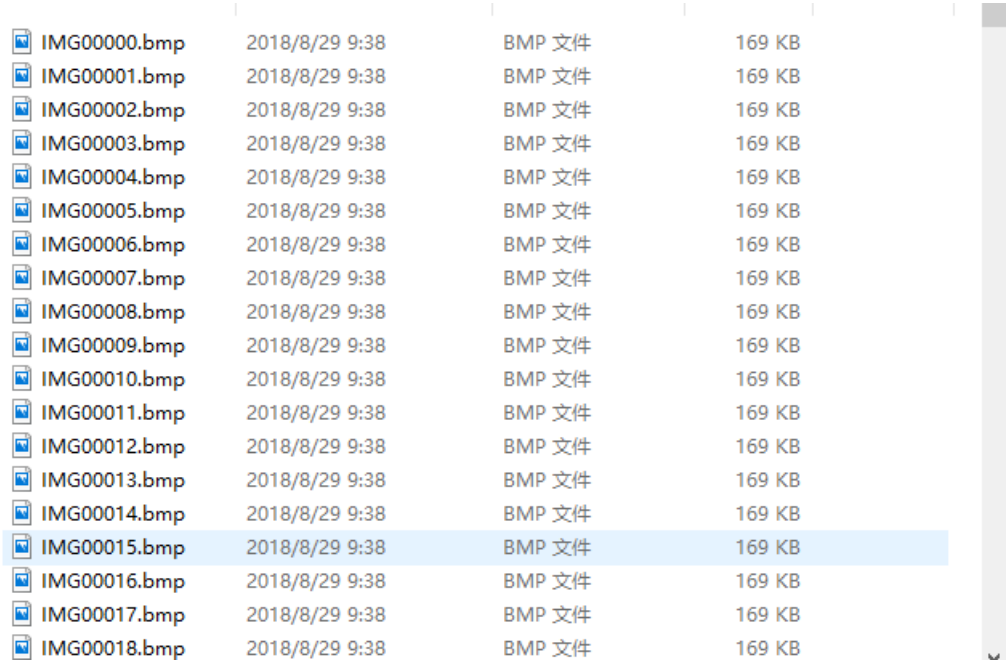
到binwalk分析一下，分离出图片



上面写着key，可能下面用得到，继续分析这张图片无异常

接着分离一下gif，分离出576张图片，是24²，难道是二维码？苦逼的画完二维码后，这什么东西？





移位移半天也没组合出一个像样的二维码，看来不是了，那两个变量还能代表什么，应该是0，1了。

按照紫色1，绿色0的规则排列出了以下数据：

```
0110111100111000010001000110110001111000010010110010101101001000001110000111011101110011011010010101100001100101001011110100010101010010010001100111000001000001010011010110000101000010010100000110100101001001011000110110101000110001011100110100100001111001010001110100111101001101011011010101000101000100011010110100101100101011011101010101100001110011010101100101101001100111011100100110010100110101010001000101001101011000011101110011110100111101011010000110100001101000011010000110100001101000011010000110100001101000011010000110100001101000011010000110100001101000011010000110100001101000
```

按照紫色0，绿色1的规则排列出以下数据：

```
1001000011000111101110111001001110000111101101001101010010110111110001111000100010001100100101101010011110011010110100001011101010101101101110011000111110111111010110010100111101011110110101111100101101011011010011100100101011100111010001100101101111000011010111000101100001011001010010010101011101011101110010100101101001101010010001010101001111000110010101001101001011001100010001101100110101100101010111011101011001010011110001000110000101100001010010111100101111001011110010111100101111001011110010111100101111001011110010111100101111001011110010111100101111001011110010111100101111001011110010111
```

与ASCII码表(表见下)比对发现紫色1，绿色0的数据可翻译为编码格式：

o8DIxK+H8wsiXe/ERFpAMaBPiIcj1sHyGOMmQDkK+uXsVZgre5DSXw==hhhhhhhhhhhhhhh

ASCII可显示字符

二进制	十进制	十六进制	图形
0010 0000	32	20	（空格）(␠)
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$

二进制	十进制	十六进制	图形
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D

二进制	十进制	十六进制	图形
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d

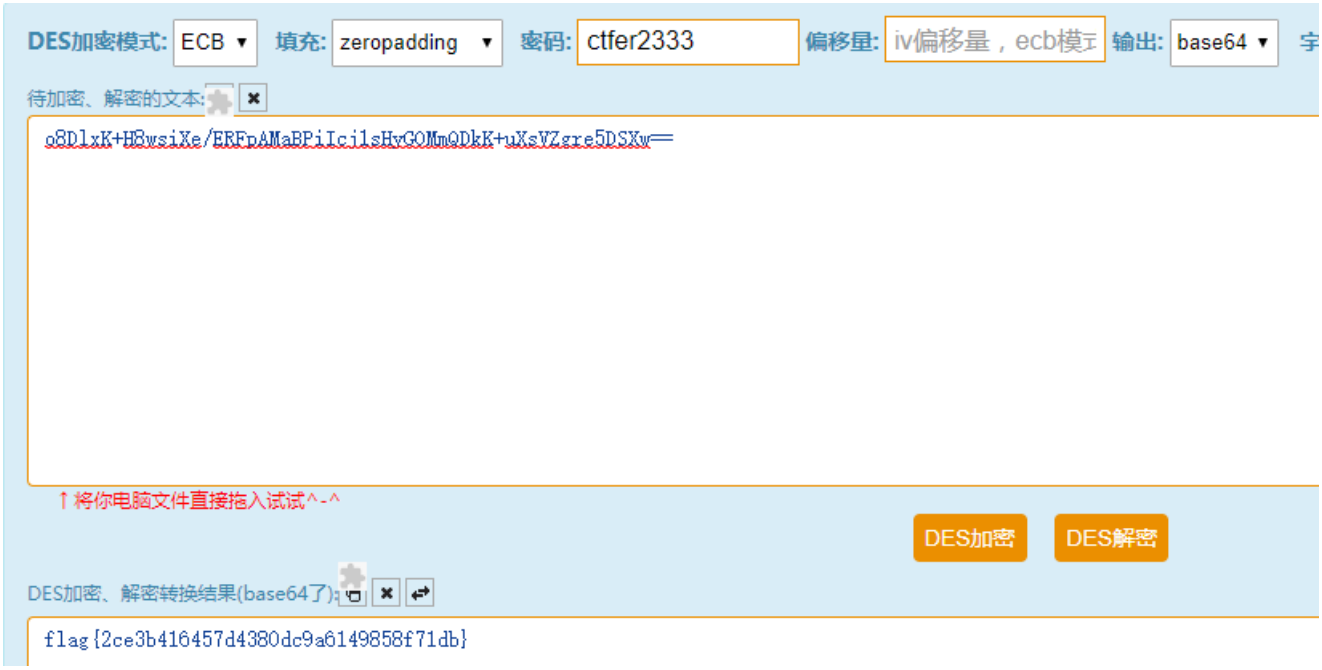
二进制	十进制	十六进制	图形
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

二进制	十进制	十六进制	图形
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

二进制	十进制	十六进制	图形
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

这应该是des加密或者base64，但是有提示key，所以应该是des加密，key是上面的图片内容，正常来说des结尾是=，这一堆h去掉就好了。

到http://tool.chacuo.net/cryptdes解密



得到flag为：flag{2ce3b416457d4380dc9a6149858f71db}